Audit Report

YEAR 2000 ISSUES WITHIN THE U.S. PACIFIC COMMAND'S
AREA OF RESPONSIBILITY
STRATEGIC COMMUNICATIONS ORGANIZATIONS

Report No. 99-126   April 6, 1999

Office of the Inspector General
Department of Defense

ARI 99-11- 2138

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Year 2000 Issues Within the U.S. Pacific Command's Area of Responsibility - Strategic Communications Organizations

B. DATE Report Downloaded From the Internet: 08/23/99

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): OAIG-AUD (ATTN: AFTS Audit Suggestions) Inspector General, Department of Defense 400 Army Navy Drive (Room 801) Arlington, VA 22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by: DTIC-OCA, Initials: __VM__ Preparation Date 08/23/99

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.

19990824 132

Acronyms

NAVCOMTELCOM	Naval Computer and Telecommunications Command
NCTAMS-PAC	Naval Computer and Telecommunications Area Master Station-Pacific
PACOM	U.S. Pacific Command
Y2K	Year 2000

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202

April 6, 1999

MEMORANDUM FOR COMMANDER IN CHIEF, U.S. PACIFIC COMMAND
ASSISTANT SECRETARY OF THE NAVY (FINANCIAL
MANAGEMENT AND COMPTROLLER)
AUDITOR GENERAL, DEPARTMENT OF THE ARMY

SUBJECT: Audit Report on Year 2000 Issues Within the U.S. Pacific Command's
Area of Responsibility-Strategic Communications Organizations
(Report No. 99-126)

We are providing this report for your review and comment. This is a follow-on
audit to Inspector General, DoD, Report No. 99-031, "U.S. Pacific Command Year
2000 Issues," November 3, 1998. The Commander in Chief, U.S. Pacific Command,
Commander, U.S. Army Pacific, and the Commander, U.S. Pacific Fleet did not
respond to the draft report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly.
We request that the Commander in Chief, U.S. Pacific Command provide comments on
the final report on Recommendation 1. We also request that the Commander, U.S.
Army Pacific and the Commander U.S. Pacific Fleet provide comments on
Recommendation 2. The comments should be provided by May 6, 1999.

We appreciate the courtesies extended to the audit staff. Questions on the audit
should be directed to Mr. Robert M. Murrell at (703) 604-9210 (DSN 664-9210)
(rmurrell@dodig.osd.mil) or Ms. Nancee K. Needham at (703) 604-8974
(DSN 664-8974) (nkneedham@dodig.osd.mil). See Appendix B for the report
distribution. The audit team members are listed inside the back cover.

Robert J. Lieberman
Assistant Inspector General
for Auditing

Report No. 99-126
(Project No. 8CC-0049.03)

April 6, 1999

Year 2000 Issues Within the U.S. Pacific Command's Area of Responsibility

Strategic Communications Organizations

Executive Summary

Introduction. This is one in a series of reports being issued by the Inspector General, DoD, in accordance with an informal partnership with the Chief Information Officer, DoD, to monitor DoD efforts to address the year 2000 computing challenge. For a list of audit projects addressing the issue, see the year 2000 web page on the IGnet at http://www.ignet.gov.

The Naval Computer and Telecommunications Area Master Station-Pacific located in Wahiawa, Hawaii, provides operational direction and management to all Naval Computer and Telecommunications System assets in the Pacific area of responsibility. The Naval Computer and Telecommunications Area Master Station-Pacific satellite earth station is the primary DoD communications installation in the Pacific and is the Navy's largest communication station providing fleet and joint support. U.S.S. *Blue Ridge* (LCC-19), home ported in Yokosuka, Japan, is the flagship of the U.S. Seventh Fleet. *Blue Ridge* functions as a Joint Task Force command ship whose mission is to serve as a command, control, communications, computers, and intelligence platform. The 58th Signal Battalion located on the island of Okinawa, Japan, provides global command, control, communications, information technology, and logistics support to joint Service warfighters. Under the control of the Joint Chiefs of Staff, the Battalion operates and maintains control of the Joint Chiefs of Staff-Pacific contingency satellite earth station and two fixed satellite earth terminals.

Objectives. The overall audit objective was to evaluate whether the U.S. Pacific Command had adequately planned for and managed year 2000 risks to avoid undue disruption to its mission. Specifically, we reviewed year 2000 risk assessments, contingency plans for mission-critical systems, and continuity of operations plans to perform core mission requirements of selected organizations within the U.S. Pacific Command's area of responsibility. The review included major DoD communications systems operated within the U.S. Pacific Command's area of responsibility.

Results. During September through December 1998, the efforts to address the year 2000 problem at the Naval Computers and Telecommunications Area Master Station-Pacific, aboard U.S.S. *Blue Ridge*, and at 58th Signal Battalion varied in scope and were evolving. Those organizations still needed to establish year 2000 action plans, develop

definitive risk-reduction strategies, conduct risk assessments of the potential impact of the year 2000 problem on operations, appoint year 2000 working groups, complete the identification and inventory of global and non-global systems, complete the assessments of year 2000 compliance and the prioritization of mission-critical systems, develop contingency plans and continuity of operations plans, and identify and report resource requirements to implement year 2000 efforts. As a result, assurance of timely and complete year 2000 conversion was still incomplete. The instability of the international political situation in portions of the Pacific rim makes it vital for U.S. Pacific forces to have a particularly vigorous and effective year 2000 conversion program.

Summary of Recommendations. We recommend that the Commander in Chief, U.S. Pacific Command ensure that adequate guidance is disseminated to all operational users involved in the year 2000 effort, and require Component commands to assist in this effort. In addition, we recommend that the Commander, U.S. Army Pacific and Commander, U.S. Pacific Fleet closely monitor, and where necessary, actively assist subordinate commands' efforts to complete risk assessments, identify and inventory global and non-global systems, assess year 2000 compliance, prioritize mission-critical systems, and develop or obtain contingency and continuity of operations plans.

Management Comments. We provided a draft of this report on February 5, 1999. The Commander in Chief, U.S. Pacific Command, Commander, U.S. Army Pacific, and the Commander, U.S. Pacific Fleet did not respond to the draft report. We request that the Commander in Chief, U.S. Pacific Command; the Commander, U.S. Army Pacific; and Commander, U.S. Pacific Fleet provide written comments on the final report finding and recommendations by May 6, 1999.

Table of Contents

Background

This report is the fourth in a series resulting from our audit of "Year 2000 Issues Within the U.S. Pacific Command's Area of Responsibility." The report discusses year 2000 (Y2K) issues at three selected strategic communications organizations located within the U.S. Pacific Command. Report No. 99-085, "Hawaii Information Transfer System," February 22, 1999, discussed the successful efforts of program managers to ensure Y2K compliance for the Hawaii Information Transfer System. Report No. 99-086, "III Marine Expeditionary Force," February 22, 1999, discussed the successful efforts of III Marine Expeditionary Force leadership to implement Y2K efforts. Report No. 99-125, "U.S. Forces Korea," April 7, 1999, discussed the Y2K level of effort within U.S. Forces Korea and its Component commands.

Executive Order No. 13073, "Year 2000 Conversion," February 4, 1998, mandates that Federal agencies do what is necessary to ensure that no critical Federal program experiences disruption because of the Year 2000 (Y2K) computing problem. The Executive Order also requires the head of each agency to ensure efforts to address the Y2K problem receive the highest priority.

The DoD target completion date for implementing Y2K compliant mission-critical systems was December 31, 1998. The DoD Y2K Management Plan stipulates the criteria for DoD Components to determine the appropriate Y2K phase for each system. Each phase of the management process represents a major Y2K program activity or segment. Target completion dates range from December 1996 through March 1999. Each system must meet defined criteria before proceeding into the next phase.

The Secretary of Defense issued the memorandum "Year 2000 Compliance" on August 7, 1998, and stated that the Y2K computing problem was a "critical national defense issue." He directed the Joint Chiefs of Staff to develop a Joint Y2K operational evaluation program and each of the Unified Commanders in Chief to review the status of Y2K implementation within his command and the command of subordinate Components. On August 24, 1998, the Deputy Secretary of Defense directed that the Military Departments provide plans for Y2K-related end-to-end testing of their respective functional processes by November 1, 1998. Public Law 105-271, "Year 2000 Information and Readiness Act," October 19, 1998, is intended to encourage the disclosure and exchange of information about computer processing problems, solutions, test practices, test results, and related matters in connection with the transition to the Year 2000.

U.S. Pacific Command. The U.S. Pacific Command (PACOM) is the largest of the nine unified commands in the Department of Defense. The PACOM area of responsibility includes 50 percent of the earth's surface and two-thirds of the world's population. It encompasses more than 100 million square miles, stretching from the west coast of North and South America to the east coast of Africa, and from the Arctic in the north to the Antarctic in the south. It also

includes Alaska, Hawaii, and eight U.S. territories. The overall mission of PACOM is to promote peace, deter aggression, respond to crises, and, if necessary, fight and win to advance security and stability throughout the Asia-Pacific region.

The PACOM, located at Camp H.M. Smith, Hawaii, is supported by Component commands from each Service: U.S. Army Pacific, U.S. Pacific Fleet, Marine Forces Pacific, and U.S. Pacific Air Forces. In addition, PACOM exercises combatant control over four sub-unified commands within the region. The sub-unified commands are U.S. Forces Japan, U.S. Forces Korea, Alaskan Command, and Special Operations Command Pacific.

Naval Computer and Telecommunications Area Master Station – Pacific.
The Naval Computer and Telecommunications Area Master Station-Pacific (NCTAMS-PAC), located in Wahiawa, Hawaii, provides operational direction and management to all Naval Computer and Telecommunications System assets in the NCTAMS-PAC area of responsibility and is the home of the Pacific Regional Commander for all Naval Computer and Telecommunications System assets. The NCTAMS-PAC satellite earth station is the primary DoD communications installation in the Pacific and is the Navy's largest communication station providing fleet and joint support.

NCTAMS-PAC manages, operates, and maintains Defense Communications System assets; and provides a full range of automated data processing and information resource services to the Navy and other DoD activities in the Pacific. NCTAMS-PAC acts as the on-island executive agent for the Oahu Telephone System and Hawaii Information Telephone Systems. Core services include Navy command, control, communications, computers, and intelligence support; Ground Mobile Force gateway; the Automatic Digital Network switching center; Mobile Satellite System; and the Global Broadcast System.

U.S.S. *Blue Ridge*. U.S.S *Blue Ridge* (LCC-19), home ported in Yokosuka, Japan, is the flagship of the U.S. Seventh Fleet. *Blue Ridge* functions as a Joint Task Force command ship whose mission is to serve as a command, control, communications, computers, and intelligence platform. Depending on the scenario, the ship can operate as a command ship for a fleet commander, naval Component commander, amphibious task force commander, joint task force commander, or as an enabling platform for a variety of other Service Component commanders.

Blue Ridge provides requisite accommodations, facilities, and support for the operation and maintenance of command, control, communications, computers, and intelligence systems and equipment. *Blue Ridge* utilizes her "main battery" of computers, communications equipment, and other electronic facilities to fulfill her mission of command and control coordination.

The ship's Joint Maritime Command Information system consists of numerous powerful computers through which information and data from worldwide sources are entered into a central database. This single integrated database concentrates the available information into a complete tactical picture of air, surface, and subsurface contacts; enabling the command element to quickly assess and concentrate on any situation which might arise. This ability to access information from military and civilian sources throughout the world gives *Blue Ridge* a global command and control capability unparalleled in Naval history. In addition, an extremely refined communications system is integral to the ship. Through an automated patch panel and computer-controlled switching matrix, any desired combination of communications equipment may be quickly connected.

58th Signal Battalion. The 58th Signal Battalion (the Battalion), located on the island of Okinawa, Japan, provides global command, control, communications, information technology, and logistics support to joint-Service warfighters. Under the control of the Joint Chiefs of Staff, the Battalion operates and maintains control of the Pacific theater contingency satellite earth station and two fixed satellite earth terminals. The Battalion operates and maintains the Army's portion of the Defense Communications System on Okinawa, in support of all DoD and non-DoD organizations located on the island, and interbase communications to the DoD on Okinawa. The Battalion also provides support for Defense Switched Network switchboards, Defense Information Services Network router nodes, Integrated Joint Communications System island-wide fiber optic and microwave links, and technical control facilities.

Objectives

The overall audit objective was to evaluate whether the PACOM had adequately planned for and managed Y2K risks to avoid undue disruption to its mission. Specifically, in this segment of the audit we reviewed Y2K risk assessments, contingency plans for mission-critical systems, and continuity of operations plans to perform core mission requirements of the NCTAMS-PAC, *Blue Ridge*, and the Battalion. The review included major DoD communications systems operated within the PACOM area of responsibility. See Appendix A for a discussion of the audit scope and methodology and a summary of prior coverage.

Status of Year 2000 Issues at Selected Strategic Communications Organizations

The efforts to address the year 2000 problem at NCTAMS-PAC, aboard *Blue Ridge*, and at the Battalion varied in scope and were evolving during the period of our review. Those organizations generally still needed to:

- establish Y2K action plans and develop definitive risk reduction strategies;

- conduct risk assessments of the potential impact of the Y2K problem on operations;

- appoint Y2K working groups;

- complete the identification and inventory of global and non-global systems;

- complete the assessments of Y2K compliance and to prioritize mission-critical systems;

- develop contingency plans and continuity of operations plans; and

- identify and report resource requirements to implement Y2K efforts.

These tasks were not completed because adequate DoD, Military Department, and PACOM guidance was not promptly disseminated and, therefore, subordinate organizations did not effectively and promptly implement Y2K corrective actions; and because system operators did not always receive information on the Y2K status of systems or remediation schedules. As a result, assurance of timely and complete Y2K conversion for those organizations was still incomplete as of late 1998. The instability of the international political situation in portions of the Pacific rim makes it vital for U.S. Pacific forces to have a particularly vigorous and effective year 2000 conversion program.

Initial Y2K Conversion Actions

NCTAMS-PAC, *Blue Ridge*, and the Battalion had taken initial actions to address Y2K problems.

NCTAMS-PAC. NCTAMS-PAC had appointed a Y2K point of contact and was trying to obtain information from system program offices and multiple Navy web sites. In addition, NCTAMS-PAC and the Defense Information Systems Agency (the Hawaii Information Transfer System program managers) recognized the need for Y2K contract clauses and procedures to ensure Y2K compliance for the program. The Hawaii Information Transfer System will provide enhanced information transfer capabilities to DoD and certain other authorized users in the State of Hawaii, and will also provide interface with other DoD and public networks at designated gateways for worldwide access. Once fully implemented, it will replace the Hawaii Area Wideband System, the Oahu Telephone System, the Defense Information System Network-Near Term and various other dedicated services in the State of Hawaii. The Hawaii Information Transfer System contractor was required to ensure that all hardware and software assets were Y2K compliant and the contract specified that there could be no additional charges to the Government for Y2K upgrades.

The *Blue Ridge*. *Blue Ridge* had appointed a Y2K point of contact. System operators on the ship were beginning the process of inventorying all electronic equipment that could be susceptible to Y2K vulnerabilities. The equipment identified was to be entered into a database and the status was to be reported monthly to higher headquarters.

The Battalion. The Battalion, in conjunction with the 10th Area Support Group, had established a Y2K steering committee and working group to address Y2K issues for all Army activities on Okinawa. The Battalion had appointed a Y2K point of contact and was in the process of evaluating information technology, communications, satellite, and network systems for Y2K compliance. The Battalion was working with various program managers to resolve Y2K issues for standard Army systems.

Sufficiency of Y2K Management Plans and Strategies

The sufficiency of Y2K conversion plans and risk reduction strategies at NCTAMS-PAC, aboard *Blue Ridge*, and at the Battalion varied in scope but generally needed improvement. Further, none of those organizations had conducted a risk assessment of the potential impact of the Y2K problem on their operations.

NCTAMS-PAC. The Department of the Navy, "Year 2000 Action Plan," September 1998, provides guidance for planning and implementation of Y2K compliance for all information technology software and systems in the Department of the Navy that face a "Y2K problem." The Action Plan is aimed at management officials and the operators who must rely on those systems. The plan describes the various phases, and action deadlines, and documentation required to solve the problem.

Nevertheless, NCTAMS-PAC had not established a Y2K action plan, developed a definitive Y2K strategy, or appointed a Y2K working group. NCTAMS-PAC higher headquarters, the Navy Computer and Telecommunications Command (NAVCOMTELCOM) had been appointed as the primary liaison for coordinating Y2K corrective actions and testing with multiple organizations. The Y2K Management plan used by NCTAMS-PAC was provided by the NAVCOMTELCOM on May 28, 1998. The plan centralized reporting, assessment, and planning for corrective action at NAVCOMTELCOM.

Blue Ridge. *Blue Ridge* had not established a Y2K action plan, developed a definitive Y2K strategy, or appointed a Y2K working group. Further, *Blue Ridge* had not received any guidance from Headquarters, U.S. Pacific Fleet. The system operators on the ship had access to four web sites that provided guidance and information on the status of systems, however, there was little evidence that the web sites were being queried for information by the system operators.

The Battalion. The Army Y2K Steering Committee issued the "Army on Okinawa Direction and Guidance Plan for Resolving The Year 2000 Problem," July 20, 1997. That plan supplements the "U.S. Army Project Change Century Action Plan," October 4, 1996, and requires the Battalion and subordinate and tenant commands to appoint a Y2K point of contact, identify and prioritize mission-critical systems, execute Y2K corrections, and establish viable contingency plans. The Battalion had begun to identify mission-critical systems.

Identification and Prioritization of Global Systems

NCTAMS-PAC, *Blue Ridge*, and the Battalion did not own the global[1] information and communications systems located and operated at their facilities. The global systems were owned and managed by various DoD Components, through program or system managers generally located in the Continental United States. As such, the three organizations we visited depended on those various DoD Components to ensure mission capability of the global systems. At those three organizations, the identification of those global systems was not complete, the assessments of Y2K compliance were not complete, and the mission-critical systems had not been prioritized. Further, decisions made by the DoD Component program managers as to whether a global system was mission-critical were made without the input of PACOM operational users and, in some cases, the operational user did not agree with the program manager determination.

---

[1] generally systems deployed at multiple DoD Component organizations and locations

NCTAMS-PAC. NCTAMS-PAC was in the assessment phase at the time of our visit. NCTAMS-PAC and NAVCOMTELCOM personnel had contacted the system owners and contractors to obtain information on mission-critical systems and the Y2K status of those systems. The Space and Naval Warfare Systems Command provided about two-thirds of the mission-critical systems to NCTAMS-PAC while NAVCOMTELCOM, the Defense Information Systems Agency, the Army Communications and Electronics Command, and the Air Force provided about one-third. The system owners had identified the mission-critical systems and determined whether those systems were Y2K compliant.

The Space and Naval Warfare Systems Command provided information on 24 systems, of which 20 were determined to be mission-critical by that command. Operations personnel at NCTAMS-PAC did not agree with all of the determinations. Assessments had been completed on four of those systems and those systems were considered to be Y2K compliant. NAVCOMTELCOM provided information on eight systems, of which two were mission-critical. The assessments were complete on all eight systems. Four of the systems were assessed as Y2K compliant and four systems were scheduled to be replaced by June 1999. The Defense Information Systems Agency, Army Communications and Electronics Command, and the Air Force program offices provided information on 15 systems, of which seven were mission-critical. The assessments were complete on all 15 systems. Nine of the systems were assessed as Y2K compliant and six systems were scheduled to be repaired or replaced.

Blue Ridge. Personnel on *Blue Ridge* were unaware of the status of their mission-critical systems. The system owners and managers had not provided a list of their mission-critical systems to *Blue Ridge* and had not provided the status of the system assessments.

The Battalion. The Battalion was in the process of completing an inventory of systems, designating the systems as mission critical or nonmission critical, and obtaining information on the Y2K compliance of those systems. The Battalion had identified and completed assessments on 38 mission-critical systems. Thirty-three of those were global systems and 21 were determined to be Y2K compliant. Twelve systems were going to be repaired or replaced.

Identification and Prioritization of Non-Global Systems

NCTAMS-PAC, *Blue Ridge*, and the Battalion owned the non-global[2] information and communications systems located and operated at their facilities. As such, the three organizations we visited were responsible to ensure mission capability of their non-global systems. At those three organizations, the

---

[2] generally facilities or local systems procured and used at an organization and its locations

identification of non-global systems was not complete, the assessments of Y2K compliance were not complete, and the prioritization of mission-critical systems had not been established.

NCTAMS-PAC. NCTAMS-PAC personnel were in the assessment phase of their infrastructure systems and equipment. They had inventoried 816 items such as generators; elevators; boilers; chemical feeds; fire and security systems; and underground storage monitoring systems; and determined that 98 were compliant. In addition, NCTAMS-PAC had sent out 71 letters to vendors questioning Y2K status of the systems (only 25 responses were received) and personnel were searching the internet and technical manuals for available Y2K data on those systems.

NCTAMS-PAC had also completed the assessment of the eight Navy base telephone switches in the NCTAMS-PAC region. Switch renovations were expected to be complete by July 1999. Further, NAVCOMTELCOM had inventoried over 600 items of personal computer and local area network equipment and was in the process of assessing Y2K compliance of those items.

Blue Ridge. *Blue Ridge* personnel had been tasked by the Commander, Naval Surface Force, U.S. Pacific Fleet, to conduct a ship-wide space-by-space, equipment-by-equipment inventory. They were to identify all electronic equipment that could be susceptible to Y2K vulnerabilities. The inventory was in process during our visit.

The Battalion. The Battalion inventoried their systems in three phases. Phase one identified computer and network hardware and software. Phase two identified satellite and communications equipment, and phase three identified non-computer equipment that requires computer-related hardware to operate. The Battalion had identified and completed assessments on five non-global mission-critical systems, of which one was determined to be Y2K compliant. Four systems were going to be repaired or replaced. In addition, the Battalion had identified 184 non-mission-critical computers, of which 128 were Y2K compliant. Forty-seven computers were going to be replaced and nine were going to be retired.

Contingency Planning

NCTAMS-PAC, *Blue Ridge*, and the Battalion had not developed Y2K contingency plans or continuity of operations plans for their systems with two exceptions. NAVCOMTELCOM had identified two systems as being mission-critical to NCTAMS-PAC and they provided Y2K contingency plans for both of those systems.

NCTAMS-PAC. The Department of the Navy, "Year 2000 Action Plan," Part IX, Contingency and Continuity of Operations Planning provides general guidance on writing plans for continuing the missions and functions during a potential Y2K failure. However, except as noted above, NCTANS-PAC was unable to provide contingency plans for any other systems and had not developed any Y2K continuity of operations plans.

Blue Ridge. Restoration plans already exist for the systems operated by the ship. However, those plans are based on common, fixable disruptions such as power outages, and not for the unpredictable failures or unpredictable restoration time that may be needed as a result of Y2K problems. The system operators had not developed any Y2K contingency plans or continuity of operations plans for *Blue Ridge.*

The Battalion. The Battalion had not developed any Y2K contingency plans or any continuity of operations plans for its systems.

Y2K Resources

NCTAMS-PAC, *Blue Ridge*, and the Battalion had not fully identified resource requirements for their Y2K efforts. Those organizations had initially been told that there would not be any additional staffing or funding for Y2K repairs and replacements and that the funding would have to be taken out of existing operations and maintenance funds. However, those organizations had not determined their requirements, analyzed their ability to realign resources to meet those requirements, or advised higher command levels of program impact.

Dissemination of Y2K Guidance and Information to Subordinate Commands

DoD, Military Department, and PACOM guidance was not adequate nor was it promptly disseminated, and system operators did not always receive information on the Y2K status of systems or remediation schedules. Therefore, the organizations that we reviewed were lagging in Y2K conversion activity.

Dissemination of Guidance. Personnel at NCTAMS-PAC, aboard *Blue Ridge*, and at the Battalion; and in some cases at higher levels, did not think that they were being given adequate guidance to perform their assigned Y2K responsibilities. Further, the guidance for the preparation of contingency plans and continuity of operations plans was not adequate because it was not specific as to which organization should prepare the plans and did not provide instructions for writing the plans. At the time of our visit, those organizations had not been provided all of the necessary Y2K guidance. At each of the three

sites visited, operators were struggling with the definition of their role in the Y2K problem and this hampered the effective and prompt implementation of the existing DoD, Military Department, and PACOM guidance that they had received. For example, those organizations did not effectively or promptly implement guidance to inventory non-global systems and infrastructure or identify and prioritize the mission criticality of those systems. The operators were confused and frustrated about what their actions should be in the Y2K effort and, consequently, were relying on others to take the lead in identifying, tracking, and resolving Y2K issues. Operations personnel did not understand clearly what needed to be done.

DoD, Military Department, and PACOM guidance for implementation of the remediation of Y2K efforts did not encompass all user functions and although the guidance assigns responsibility to various organizations, the guidance was not always coordinated among the user community. For example, guidance was not in place to ensure coordination of the identification of global mission-critical systems through operational users' input or the prioritization of those global mission-critical systems.

Dissemination of Information. Personnel at NCTAMS-PAC, aboard Blue Ridge, and at the Battalion were attempting to contact program managers to obtain Y2K status information for the systems used by their organizations, but were receiving few responses to their questions. Personnel at each organization were aware of multiple web sites available to query for Y2K information, however, most were not using the web sites for this purpose. Instead, most of the Y2K information on the systems used at their organizations was being collected by telephone or e-mail. Further, we found no evidence that site personnel were maintaining any documentation on the information provided. The system operators were not receiving information on Y2K status of systems or remediation schedules from PACOM or the global system program managers. PACOM and system managers need to become more proactive in identifying the compliance of their systems and providing the assessments to the system operators, and the system operators need to become proactive in obtaining that information.

Results of Navy Inspection. The Naval Inspector General issued "Final Report on Year 2000 Special Inquiry," December 21, 1998, which included results related to Y2K efforts in the Pacific Fleet communications and information technology infrastructure. The report stated: "Navy's efforts to meet the Y2K challenge are fragmented, poorly coordinated, and lack sufficient resources. Sharply improved focus on this problem, and real, rapid progress are essential, or our Service will be in serious trouble." The report further stated "Our people in the Fleet and the shore establishment have been inundated with short-fused data calls, but they receive little or no feedback on the Y2K status of the systems on which they depend."

Conclusion

The selected strategic communications organizations we visited between September and December 1998 had made some progress in addressing the Y2K problem. However, we agree with the Naval Inspector General's assessment that more guidance, information, and assistance needs to be provided to them. The instability of the international political situation in portions of the Pacific rim makes it vital for U.S. Pacific forces to have a particularly vigorous and effective year 2000 conversion program; however, insufficient progress was being made as of late 1998.

Recommendations

1. We recommend that the Commander in Chief, U.S. Pacific Command:

    a. Ensure that guidance is adequate to eliminate confusion in the assignment of responsibilities toward Y2K efforts.

    b. Ensure that guidance is disseminated to all operational users involved in the Y2K effort.

    c. Require Component commands with elements in the U.S. Pacific Command area of responsibility to:

        1. Assist the U.S. Pacific Command to ensure that guidance is adequate to eliminate confusion in the assignment of responsibilities for Y2K efforts.

        2. Assist the U.S. Pacific Command to ensure that guidance is disseminated to all operational users involved in the Y2K effort.

2. We recommend that the Commander, U.S. Army Pacific and the Commander, U.S. Pacific Fleet closely monitor and, where necessary, actively assist subordinate commands' efforts to:

    a. Complete risk assessments of the potential impact of Y2K problems on operations.

    b. Complete the identification or inventory of global and non-global systems.

    c. Complete the assessments of Y2K compliance.

d. Complete the prioritization of mission-critical systems.

e. Develop or obtain contingency and continuity of operations plans.

f. Identify and report resource requirements to implement Y2K efforts.

Management Comments Required

The Commander in Chief, U.S. Pacific Command, Commander, U.S. Army Pacific, and Commander, U.S. Pacific Fleet did not comment on a draft of this report. We request that the Commander in Chief, U.S. Pacific Command, Commander, U.S. Army Pacific, and Commander, U.S. Pacific Fleet provide comments on the final report by May 6, 1999.

Appendix A. Audit Process

This is one in a series of reports being issued by the Inspector General, DoD, in accordance with an informal partnership with the Chief Information Officer, DoD, to monitor DoD efforts to address the Y2K computing challenge. For a listing of audit projects addressing the issue, see the Y2K web page on the IGnet at http://www.ignet.gov.

Scope

We reviewed and evaluated the ability of selected strategic communications organizations in the PACOM to resolve Y2K issues to avoid undue disruption to their missions. We reviewed and evaluated DoD, Service, and Joint Staff directives, policies and processes related to Y2K activities. For this portion of the audit, we visited NCTAMS-PAC, U.S.S. *Blue Ridge*, and the Battalion. We reviewed the process employed by those organizations to inventory their systems, identify and prioritize mission-critical systems, conduct risk assessments and report the Y2K status of systems, and develop contingency or continuity of operations plans. We interviewed the leadership and members of the Y2K entities established at the sites visited. We also interviewed members of the unified command and Service Component staffs to determine each respective command's level of involvement and interest in addressing Y2K problems.

DoD-Wide Corporate Level Government Performance and Results Act Goals. In response to the Government Performance and Results Act, the Department of Defense has established 6 DoD-wide corporate-level performance objectives and 14 goals for meeting the objectives. This report pertains to achievement of the following objective and goal.

- **Objective:** Prepare now for an uncertain future.
  Goal: Pursue a focused modernization effort that maintains U.S. qualitative superiority in key war fighting capabilities. **(DoD-3)**

DoD Functional Area Reform Goals. Most major DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to achievement of the following objectives and goals in the Information Technology Management Functional Area.

- **Objective:** Become a mission partner.
  Goal: Serve mission information users as customers. **(ITM-1.2)**

- **Objective:** Provide services that satisfy customer information needs.
  Goal: Modernize and integrate DoD information infrastructure.
  (ITM-2.2)

- **Objective:** Provide services that satisfy customer information needs.
  Goal: Upgrade technology base. **(ITM-2.3)**

General Accounting Office High-Risk Area. In its identification of risk areas, the General Accounting Office has specifically designated risk in resolution of the Y2K problem as high. This report provides coverage of that problem and of the overall Information Management and Technology high-risk area.

Methodology

Audit Type, Dates, and Standards. We performed this program audit from September through December 1998 in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD. We did not use computer-processed data to perform this audit.

Contacts During the Audit. We visited or contacted individuals and organizations within DoD. Further details are available upon request.

Management Control Program. We did not review the management control program as it related to the overall audit objective because DoD recognized the Y2K issue as a material management control weakness area in the FY 1998 Annual Statement of Assurance.

Summary of Prior Coverage

The General Accounting Office and the Inspector General, DoD, have conducted multiple reviews related to Y2K issues. General Accounting Office reports can be accessed over the Internet at http://www.gao.gov. Inspector General, DoD, reports can be accessed over the Internet at http://www.dodig.osd.mil.

14

Appendix B. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)
   Deputy Chief Financial Officer
   Deputy Comptroller (Program/Budget)
Under Secretary of Defense for Personnel and Readiness
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
   Deputy Assistant Secretary of Defense (Command, Control, Communications,
      Intelligence, Surveillance, Reconnaissance, and Space Systems)
   Deputy Chief Information Officer and Deputy Assistant Secretary of Defense (Chief
      Information Officer Policy and Implementation)
   Principal Deputy-Y2K
Assistant Secretary of Defense (Public Affairs)
Director, Defense Logistics Studies Information Exchange

Joint Staff

Director, Joint Staff

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)
Auditor General, Department of the Army
Chief Information Officer, Army
Inspector General, Department of the Army

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Auditor General, Department of the Navy
Chief Information Officer, Navy
Inspector General, Department of the Navy
Inspector General, Marine Corps

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force
Chief Information Officer, Air Force
Inspector General, Department of the Air Force

Unified Commands

Commander in Chief, U.S. European Command
Commander in Chief, U.S. Pacific Command
Commander in Chief, U.S. Atlantic Command
Commander in Chief, U.S. Central Command
Commander In Chief, U.S. Special Operations Command

Other Defense Organizations

Director, Defense Information Systems Agency
    Inspector General, Defense Information Systems Agency
    Chief Information Officer, Defense Information Systems Agency
    United Kingdom Liaison Office, Defense Information Systems Agency
Director, National Security Agency
    Inspector General, National Security Agency
Inspector General, Defense Intelligence Agency
Inspector General, National Imagery and Mapping Agency
Inspector General, National Reconnaissance Office

Non-Defense Federal Organizations and Individuals

Office of Management and Budget
    Office of Information and Regulatory Affairs
General Accounting Office
    National Security and International Affairs Division
        Technical Information Center
    Accounting and Information Management Division
        Director, Defense Information and Financial Management Systems

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Government Affairs
Senate Special Committee on the Year 2000 Technology Problem
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Management, Information, and Technology,
  Committee on Government Reform
House Subcommittee on National Security, International Affairs, and Criminal Justice,
  Committee on Government Reform

Audit Team Members

The Contract Management Directorate, Office of the Assistant Inspector General For Auditing, DoD, prepared this report.

Paul J. Granetto
Robert M. Murrell
Nancee K. Needham
Peter J. Larson
Charles R. Johnson
John R. Huddleston
Elizabeth Ramos

18